RESUMO DO RELATÓRIO DA IHS INFONETICS RESEARCH

Estratégias de segurança de data center e liderança do fornecedor

Resumo

Março de 2015

Diretor de pesquisas Jeff Wilson

Índice

Lista de documentos

PONTOS PRINCIPAIS

A batalha pelo domínio da segurança de data centers segue intensa em 2015, principalmente no mercado de dispositivos de ponta. No ano de 2014 observamos mudanças importantes na participação de mercado e, como resultado, vários compradores estão avaliando fornecedores antigos e novos considerando os seguintes critérios:

- Os fornecedores têm as interfaces e o desempenho (conexão e produtividade) que os compradores exigem hoje em dia; os compradores descartarão os fornecedores em 2015 se acreditarem que a infraestrutura de segurança vai paralisar seu data center de alto desempenho; as portas 25 G, em especial, ganharão destaque rapidamente como principal produto para data center a partir de 2016.
- A melhoria do desempenho não ocorre em detrimento da eficiência da segurança e das ferramentas de gerenciamento/política; o acesso em tempo real a dados sobre ameaças encabeça a lista dos novos determinantes de investimento.
- Hoje em dia, as soluções são competitivas em termos de custo e oferecem processos de atualização atraentes, inclusive a capacidade de melhorar o desempenho por meio de atualizações de software e/ou hardware e adicionar novos mecanismos de proteção.
- Os fornecedores têm um roadmap convincente para virtualização e Software Defined Network (SDN - Redes Definidas por Software), com planos concretos para produtos, que será apresentado no final de 2015. Além disso, eles disponibilizam atualmente uma série de plataformas de controladores de hipervisor e SDN como uma prova de conceito.

A transformação mais importante que afeta os data centers corporativos hoje em dia é a adoção da tecnologia de virtualização de servidores e do software de orquestração de DC, pois eles são os componentes essenciais do data center virtualizado e fatores indispensáveis na implantação da SDN no futuro; 76% dos entrevistados consideram a virtualização um determinante importante para a aquisição de novas soluções de segurança. Ou seja, eles ainda não estão fazendo esforços para adquirir soluções de segurança compatíveis com a SDN (estão quase no final da lista de determinantes de investimento em segurança, mas são determinantes para 71% dos compradores).

Quando se trata da força da marca dos principais critérios de compra de produtos de segurança de data center, a Cisco, a McAfee, a HP, a Juniper e a VMware geralmente ocupam o topo da lista. A força nos critérios individuais é principalmente o resultado da força geral da marca (grandes fornecedores são melhores no geral), mas há alguns altos (a Juniper se sobressai em inovação tecnológica e preço) e baixos (a Cisco demonstra seu ponto fraco no preço/desempenho e também em manutenção e suporte). Já a Palo Alto apresenta uma pontuação surpreendentemente alta em gerenciamento em relação à força e à divulgação de sua marca em geral.

INTRODUÇÃO

Situação do mercado

De provedores de hospedagem de grande porte a empresas centradas na nuvem, como Google e Amazon, e empresas de grande e médio porte, os departamentos de TI no mundo todo estão consolidando e reconstruindo os data centers, movendo a infraestrutura para a nuvem e buscando arquiteturas de data center flexíveis e programáveis (como a SDN para redes de data centers) em uma iniciativa para obter a agilidade e o desenvolvimento necessários para operar seus negócios e gerenciar custos. As empresas que buscam implantar soluções de segurança em data centers devem avaliar diversos produtos de segurança, do software de servidor que protege uma única máquina (física ou virtual) a dispositivos virtuais que protegem hipervisores e, até mesmo, dispositivos de segurança big iron que estão no data center em vários locais. Há várias soluções disponíveis, mas há pouco consenso sobre qual é a melhor e quem deve fornecê-la. Operadores de data centers corporativos também buscam mudanças importantes na maneira de planejar sua infraestrutura (SDN para redes, armazenamento definido por software, implantação de software para orquestração de data center e novas arquiteturas para servidores com várias CPUs) que, com certeza, vão gerar mudanças na forma de implantar a segurança.

Então, o que os usuários finais ou as empresas que estão implantando ou atualizando seus data centers hoje em dia pensam sobre os problemas de segurança que enfrentam? Realizamos esta pesquisa para responder às principais questões sobre os planos dos compradores em relação à segurança em seus data centers.

Resumo da metodologia e dos dados demográficos

Com a ajuda de uma equipe de tomadores de decisão de TI qualificados, realizamos uma pesquisa na Web em março de 2015 com 137 empresas de médio e grande porte (mais de 500 funcionários) que operam seus próprios data centers, definidos como uma área em um prédio conectado a instalações de telecomunicações usadas para alojar servidores conectados à rede local (sistemas de computador) e sistemas de armazenamento, que geralmente engloba SANs, fontes de alimentação redundantes ou de backup, conexões de telecomunicação redundantes, controles ambientais (como ar-condicionado e extintores de incêndio) e dispositivos de segurança.

Para poder participar da pesquisa, os entrevistados tinham que ter conhecimento detalhado das soluções de segurança implantadas em seus data centers e ter influência sobre as decisões de compra dessas soluções. Todos os entrevistados são tomadores de decisão principais ou têm muita influência.

DETERMINANTES

Os entrevistados estão enfrentando vários problemas ao fazer novos investimentos em segurança para data centers. Nos últimos anos, a segurança para servidores virtualizados encabeçava a lista, mas houve uma grande mudança. Em 2015, no topo da lista, estão soluções que lançam mão da inteligência contra ameaças em tempo real e podem inspecionar o tráfego criptografado.

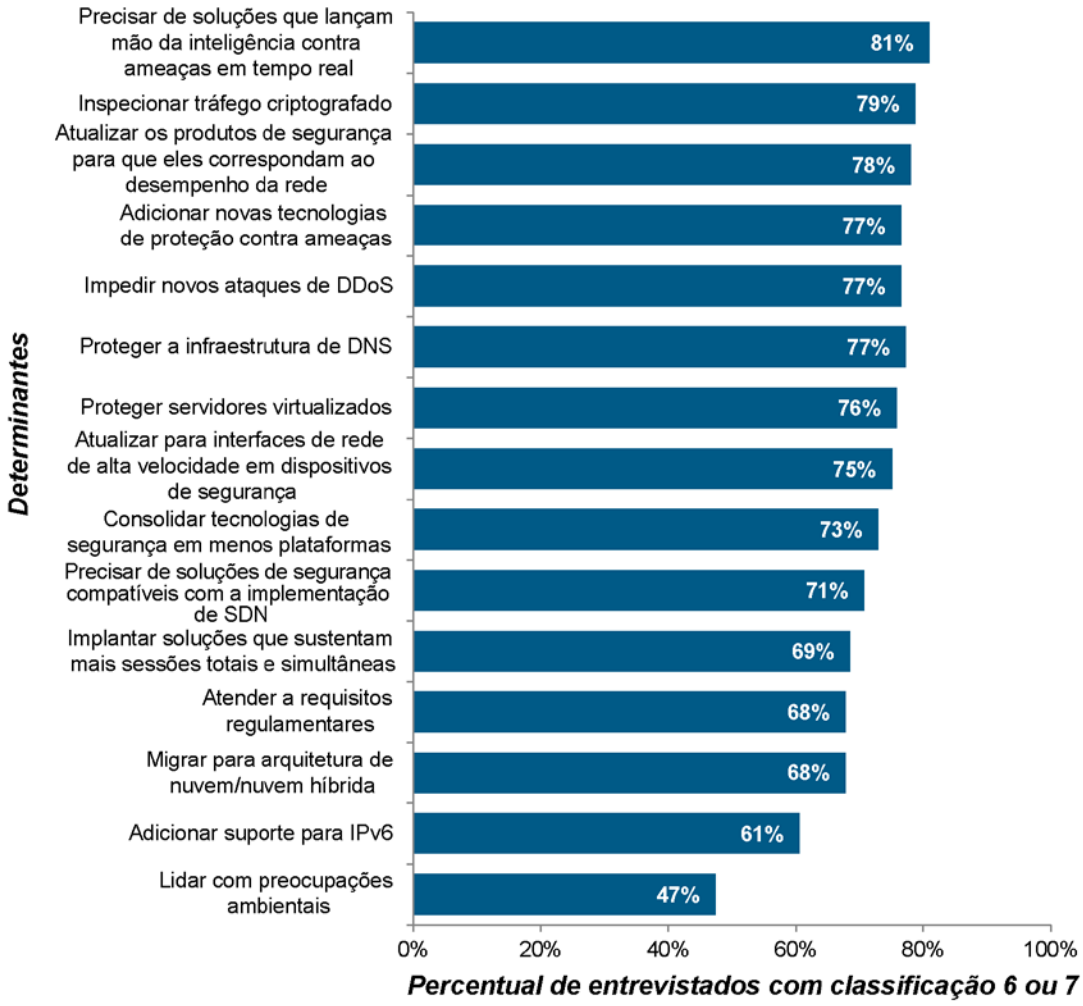
Os entrevistados classificaram a importância de vários fatores que determinam a aquisição de novas soluções de segurança para seus data centers em uma escala que varia de 1 a 7, em que 1 significa *não ser um determinante,* 4 significa ser *um determinante médio e* 7 significa ser *um determinante expressivo*. O gráfico a seguir mostra a porcentagem de entrevistados que classificaram cada recurso como 6 ou 7, ou como *um determinante.*

Quanto maior o número de ameaças de grande repercussão, mais os compradores de soluções de segurança para data center deixarão de lado as preocupações com desempenho e arquitetura e se concentrarão na essência do problema: interromper as violações prejudiciais. Os entrevistados querem contar com soluções vinculadas à inteligência contra ameaças em tempo real para reduzir sua exposição a ameaças prejudiciais, o que é difícil de conseguir com a velocidade atual dos data centers. Os fornecedores de soluções de segurança para data center devem divulgar a inteligência de ameaças e a sua conectividade, adicionando essa informação a mensagens relacionadas ao desempenho geral e à migração para SDN/NFV, uma vez que ela merece ter a mesma importância (se não mais).

Eles também desejam ter visibilidade do tráfego criptografado. Desde o caso de divulgação de informações sigilosas por Edward Snowden, houve uma grande mudança na Internet. Vários sites importantes (Facebook, Google etc.) mudaram para HTTPS de um dia para o outro e criptografaram todo o tráfego. Embora isso seja bom em termos de liberdade pessoal, é um pesadelo para a aplicação da segurança. Há diversas opções para lidar com o tráfego criptografado, da adição de cartões SSL a dispositivos atuais à implantação de uma infraestrutura de inspeção SSL global. Além disso, os compradores estão exigindo soluções de inspeção SSL que funcionarão nos data centers.

Documento 1

Novos determinantes para a aquisição de soluções de segurança de data center n=137



A transformação mais importante que afeta os data centers corporativos hoje em dia é a adoção de tecnologias de virtualização de servidor e do software de orquestração de DC, pois eles são os componentes essenciais do data center virtualizado e fatores indispensáveis na implantação da SDN no futuro. A virtualização é considerada um determinante importante para a aquisição de novas soluções de segurança para 76% dos entrevistados; a implantação de servidores virtualizados exigirá um investimento em novas soluções de segurança no data center.

Embora estejam buscando solucionar os problemas de segurança associados a servidores virtualizados, os compradores tradicionais de data centers corporativos estão apenas começando a adquirir soluções de segurança compatíveis com a SDN (parte inferior da lista, apenas classificada como determinante expressivo por 71% dos participantes). A maioria dos data centers corporativos ainda não têm infraestrutura de SDN instalada, por isso ela não representa um determinante a curto prazo para aquisições de segurança. Este ano será um ano de transição para a SDN como um determinante, sendo que 2016 será o ano em que as SDNs serão um determinante dominante na aquisição de soluções de segurança para data centers. Isso não significa que os fornecedores não devem trabalhar em suas soluções ou treinar sua base de clientes em relação à maneira como funcionarão suas soluções em um ambiente de SDN no futuro, significa apenas que atualmente o fornecimento dessa solução não é importante.

ESTRATÉGIAS DE IMPLANTAÇÃO DE SEGURANÇA NO DATA CENTER

Ao solucionar um problema de segurança no data center, os arquitetos de segurança devem atender a uma longa lista de requisitos tecnológicos e corporativos, mas as opções de produto costumam estar em três grupos básicos, independentemente de as empresas comprarem um data center mais tradicional, um data center em que alguns dos servidores e armazenamento foram virtualizados ou um data center completamente virtualizado para a implementação total da SDN.

Grandes dispositivos de alto desempenho (firewalls, IPS, DDoS etc.) ainda são necessários para proteger a infraestrutura do data center contra ataques. Os aplicativos e protocolos protegidos por esses dispositivos continuam evoluindo, e os requisitos de desempenho aumentam sem parar. Em alguns casos, dispositivos de alto desempenho podem reconhecer a virtualização e direcionar o tráfego de e para VMs e, no futuro, trabalhar até mesmo com plataformas de orquestração de SDNs e data centers.

Após o big iron, vem a ***proteção de servidores em hipervisores***. Vemos aqui nomes conhecidos (como Juniper, Check Point, Cisco, Symantec, McAfee e Trend Micro) e novos (os próprios fornecedores de plataformas de virtualização, sendo a VMware a mais ativa, e fornecedores especializados como a Catbird). As funções de segurança exatas desses produtos variam, assim como o alcance da comunicação com outros elementos de segurança, mas a maioria concorda que é necessário ter algo que possa interagir com o hipervisor e proteger várias máquinas virtuais. Com o tempo, essas plataformas também serão construídas para comportar a SDN e a orquestração de data centers.

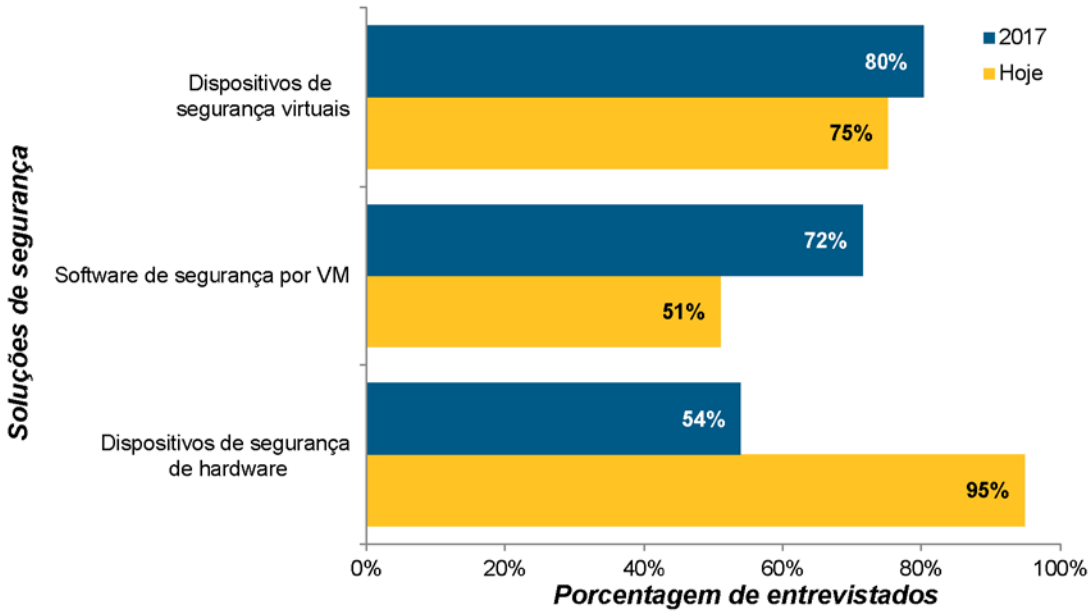
Por fim, há a ***proteção de instâncias de servidor individual***. Voltaremos a falar dos fornecedores de software de segurança tradicionais (como Symantec, McAfee e Trend Micro) que oferecem produtos com diversas funções, de AV à criptografia e gerenciamento da integridade do arquivo. Há um grande potencial de parceria entre os operadores de dispositivos e hipervisores e as empresas que oferecem proteção de servidores individuais.

Perguntamos aos entrevistados sobre sua estratégia básica para implantar soluções de segurança no data center, e eles são claramente favoráveis a uma abordagem multicamadas, tendo vários deles já implantado uma combinação de dispositivos de hardware e dispositivos virtuais. Mais da metade implanta o software de segurança no servidor por VM, apesar de ser o modelo de implantação de segurança de data center mais caro e mais difícil de gerenciar. É interessante observar que muitos entrevistados esperam reduzir o uso de dispositivos de hardware no data center nos próximos 2 anos; isso faz parte de uma mudança maior em direção à infraestrutura virtualizada, com compradores com visão de futuro que esperam obviamente soluções disponibilizadas na nuvem para impactar sua arquitetura.

Esperamos que implantações futuras de SDN mudem o equilíbrio de dispositivos de hardware e de software no data center, e quando fizermos esta pesquisa no próximo ano, esperamos que os entrevistados tenham muito mais conhecimento sobre SDN e ferramentas de orquestração de data center. Acreditamos que essa migração de hardware para software poderá ser a justificativa para as tecnologias de segurança da camada mais alta (sistema de mensagens, IPS, aplicativo, proteção da Web) e acreditamos que provavelmente sempre haverá infraestrutura de segurança de hardware para mitigação de DDoS e firewalls na borda do data center (onde ele se conecta à Internet), mesmo que essas soluções sejam virtualizadas no núcleo do data center em uma camada de serviços.

Documento 2

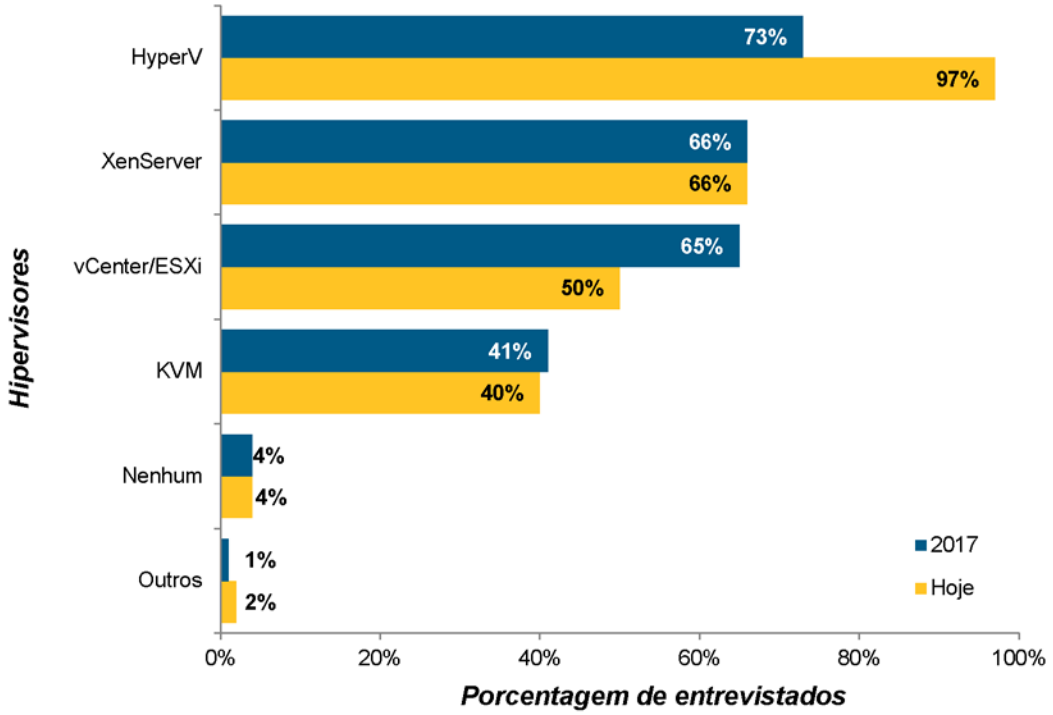
Soluções de segurança implantadas no data center n=137



A seguir, perguntamos aos entrevistados com quais plataformas de hipervisor suas soluções de dispositivos de segurança virtual precisam ser compatíveis. Atualmente, a batalha está acirrada entre 3 concorrentes no data center corporativo entre VMware (vCenter), Citrix (XenServer) e Microsoft (HyperV), embora a KVM não esteja muito distante da VMware no momento. No momento, a Microsoft leva vantagem, pois há várias empresas avaliando o HyperV e até mesmo explorando serviços de nuvem do Azure e vários provedores de serviços relatando esporadicamente que a Microsoft está fazendo um excelente trabalho técnico para tornar o HyperV o produto preferencial em um ambiente de hospedagem. Ainda estamos engatinhando no mercado de soluções de segurança virtual e realmente não há sentido em declarar um vencedor aqui; a verdade é que a maioria dos dispositivos virtuais precisará ser compatível com a grande maioria das plataformas de hipervisor.

Documento 3

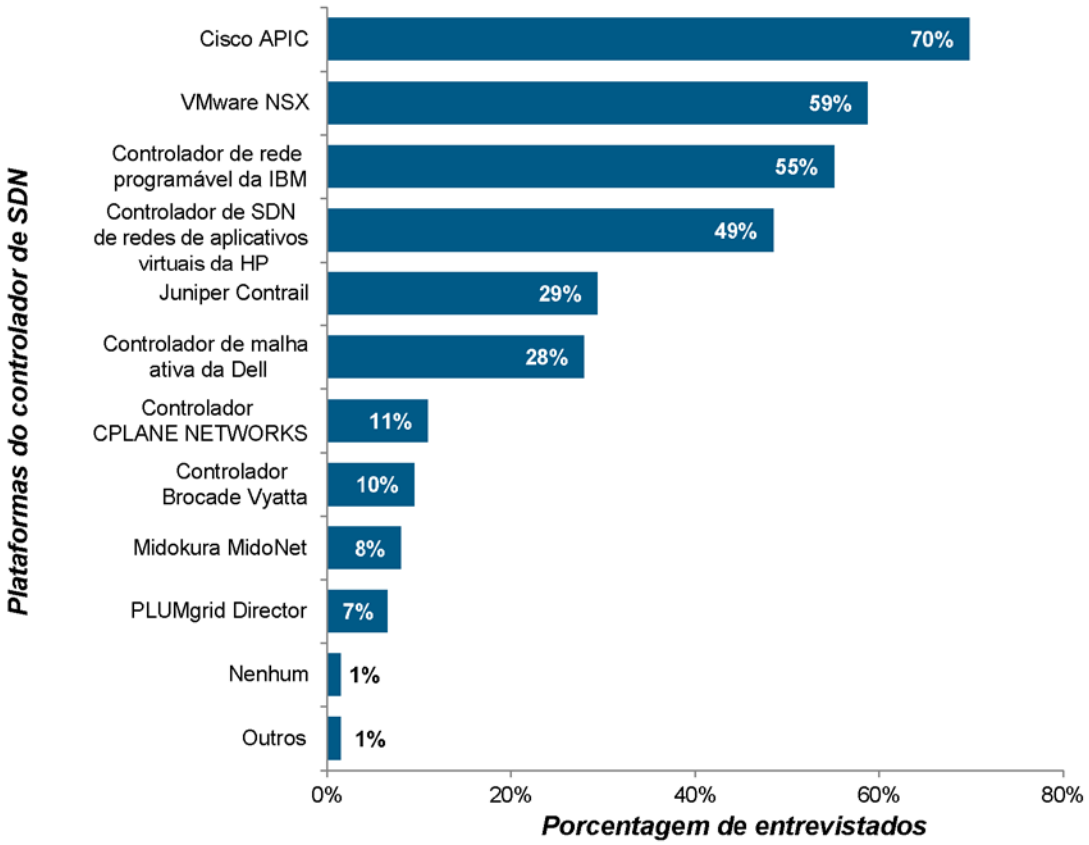
Compatibilidade do hipervisor
n=137



Após a virtualização do servidor, uma das tecnologias que deve ser implantada na maioria dos data centers corporativos será a SDN. Mais uma vez, a discussão sobre a SDN no mundo dos data centers é grande, mas na realidade ainda estamos no início do ciclo de sua implantação. Perguntamos aos entrevistados quais controladores de SDN eles estavam avaliando atualmente, e houve uma resposta equilibrada para várias plataformas, incluindo os da Cisco, VMware, IBM e HP. Na verdade, a batalha dos controladores pode ou não ter um impacto negativo na guerra da tecnologia de segurança, uma vez que a maioria dos controladores fará interface com todos os produtos dos fornecedores de segurança, embora haja implicações. É muito provável que um operador de data center que opte pelo Juniper Contrail implante dispositivos virtuais Juniper vSRX numa primeira etapa, mesmo se a longo prazo puder escolher qualquer fornecedor de segurança para seus serviços. A seleção de fornecedores de controladores pode ser um indicador de sucesso antecipado no mercado para produtos de segurança virtualizada.

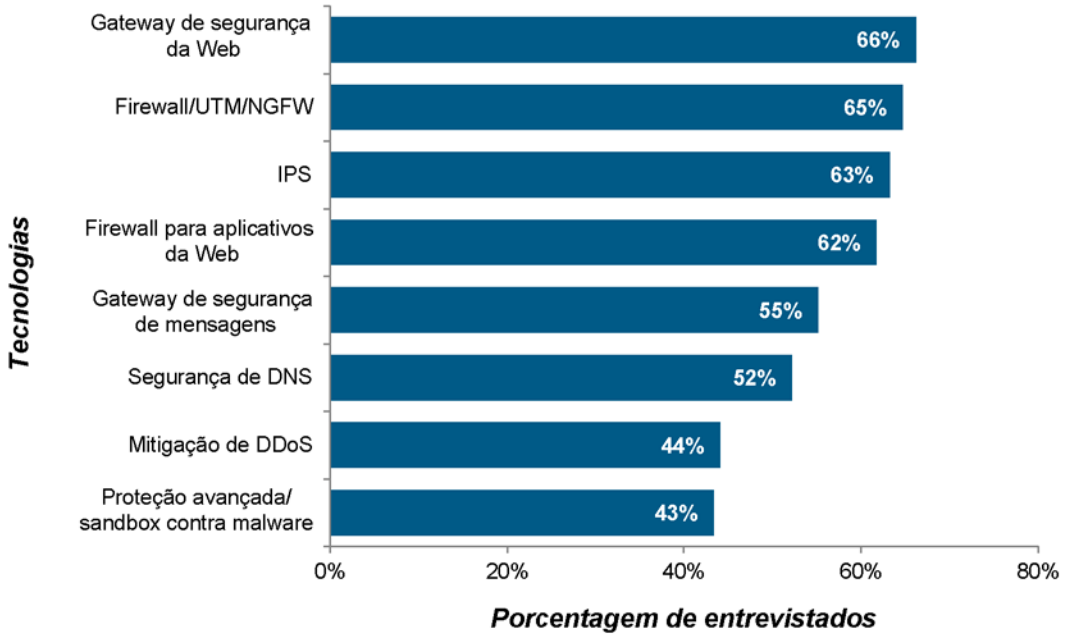
Documento 4

Plataformas de controlador de SDN em avaliação n=137



Perguntamos também aos entrevistados quais tecnologias de segurança eles planejaram implantar usando dispositivos virtuais até o final de 2015. Os 4 principais são uma combinação de rede central (firewall e IPS) e produtos de aplicativo/conteúdo (gateway de segurança da Web e WAF). É consenso que as empresas provavelmente implantarão tecnologias de camada mais alta (como SWG e WAF) em formato de dispositivo virtual, pois os próprios aplicativos já estão sendo executados em uma infraestrutura virtualizada. Ou seja, há mais ofertas de firewall virtualizado no mercado a cada dia, e à medida que as empresas virtualizarem mais a infraestrutura da rede no data center, as ferramentas de segurança de rede seguirão o mesmo caminho.

Documento 5 Tecnologias de segurança implantadas como dispositivos virtuais n=137

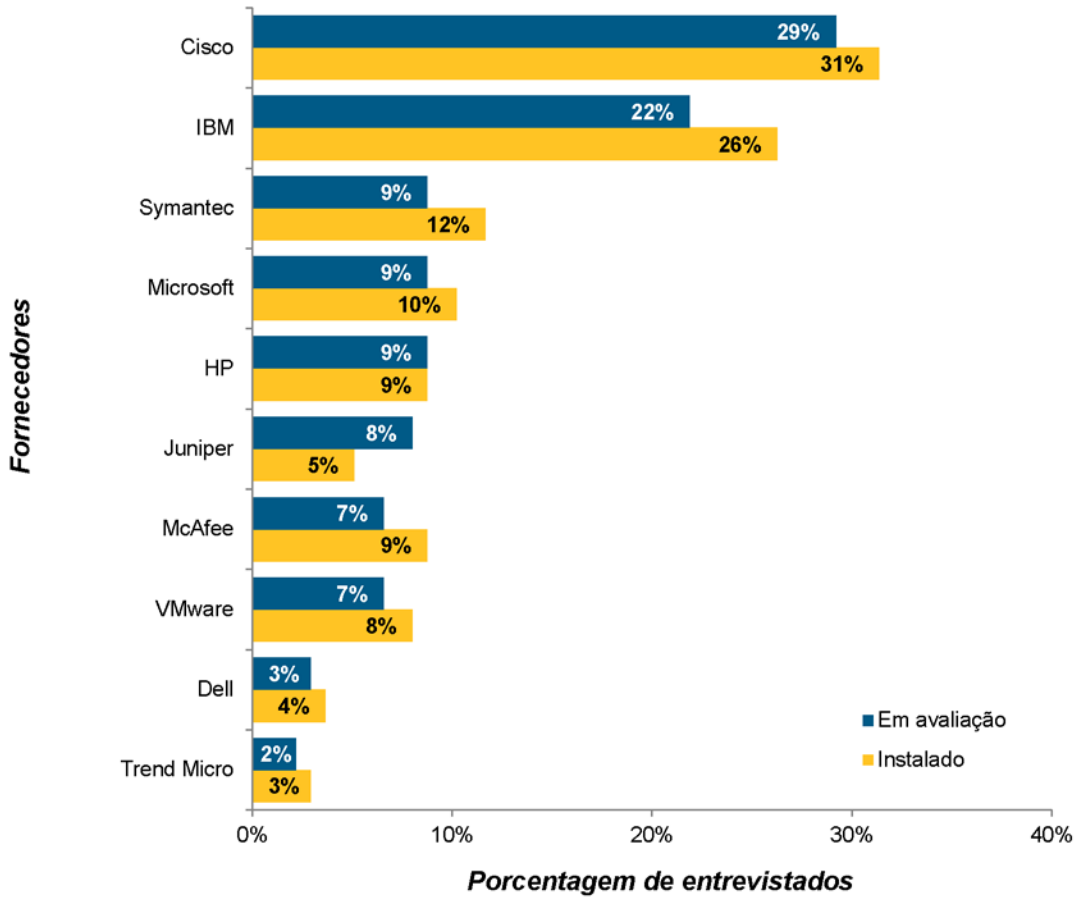


FORNECEDORES DE SOLUÇÃO INSTALADOS E EM AVALIAÇÃO

Em uma questão aberta, perguntamos aos entrevistados quais soluções de segurança de data center eles estão usando no momento e quais estão pensando em usar em 2016.

Este é um mercado fragmentado, onde os fornecedores utilizados dispõem de vários fornecedores de virtualização, de aplicativos/bancos de dados, fortes concorrentes de servidores/data centers, operadores de segurança do cliente, fornecedores de segurança de rede e fornecedores que também têm uma grande participação no negócio de integração de rede para data centers. Os fornecedores bem sucedidos provavelmente serão aqueles que se posicionam melhor em relação à liderança na segurança de data center e nuvem por meio de uma combinação dos produtos certos (com foco especial na disponibilização de atualizações de desempenho a um custo razoável), um excelente histórico de eficiência de segurança, uma oferta de soluções/integração excepcional e a capacidade de usufruir dos pontos fortes adjacentes (como a HP e a IBM apoiadas em seu negócio de servidores e armazenamento para vender segurança no data center ou a Cisco e a Juniper, criando ofertas expressivas que combinam segurança, switching e roteamento).

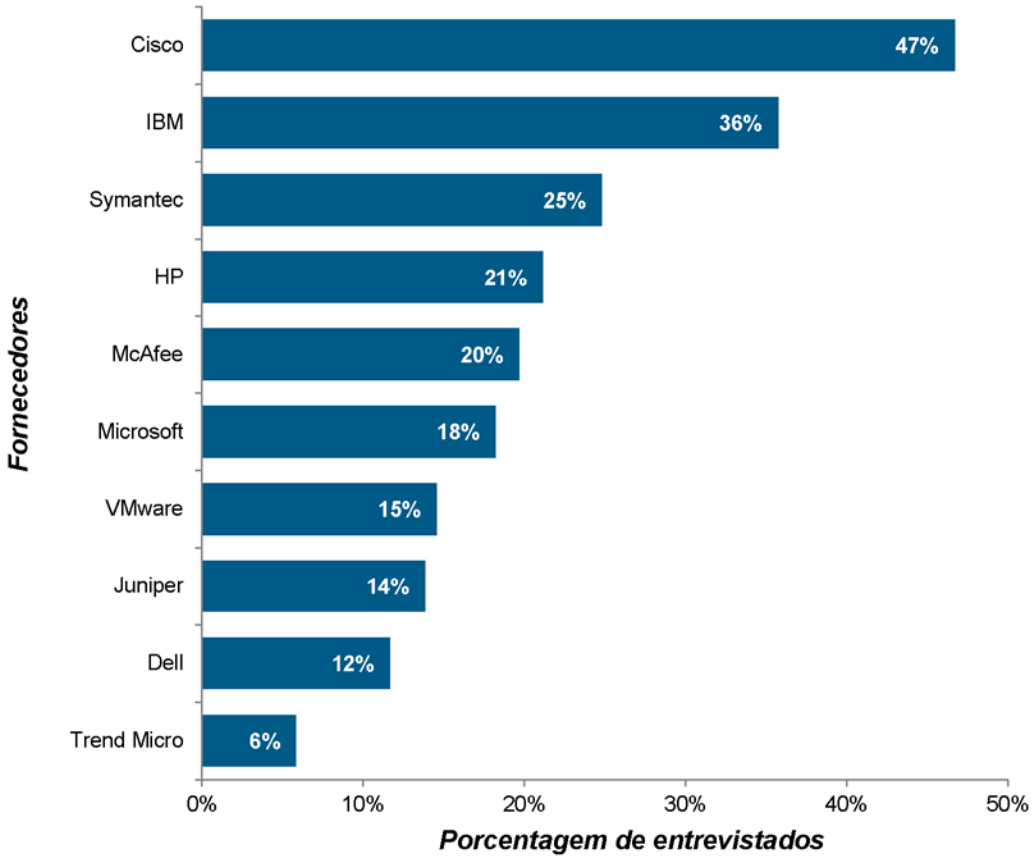
Documento 6 **Fornecedores de solução de segurança de data center instalados e em avaliação n=137**



PRINCIPAIS FORNECEDORES DE SOLUÇÕES DE SEGURANÇA DE DATA CENTER—PERCEPÇÃO DOS ENTREVISTADOS

Em uma questão aberta, perguntamos aos entrevistados quem eles consideram ser os 3 principais fornecedores de soluções de segurança para data centers, uma medida chamada *percepção da marca sem ajuda,* o que fornece uma boa visão da força geral da marca. Normalmente, quanto maior o fornecedor (que tenha, por exemplo, amplo portfólio de produtos) e quanto mais visível for sua marca (que conta, por exemplo, com comerciais de TV, disposição do produto), melhor ele se sairá nessa questão: a força global da marca supera a liderança técnica ou do produto, o que significa que a IBM, um ícone em data center por décadas, encabeça a lista, embora não tenha uma oferta de produtos tão ampla como a de outros fornecedores (seu negócio de integração significativa não prejudica a percepção da marca). No geral, a Cisco lidera, e os outros fornecedores nessa lista são as principais marcas em segurança dos consumidores (McAfee), SO/aplicativos para desktop (Microsoft) e amplas soluções de TI (HP). Empresas grandes como a VMware, fornecedores importantes de soluções de segurança de data center, ainda não conseguiram alcançar o topo da lista.

Documento 7 **Principais fornecedores de soluções de segurança de data center: percepção dos entrevistados n=137**



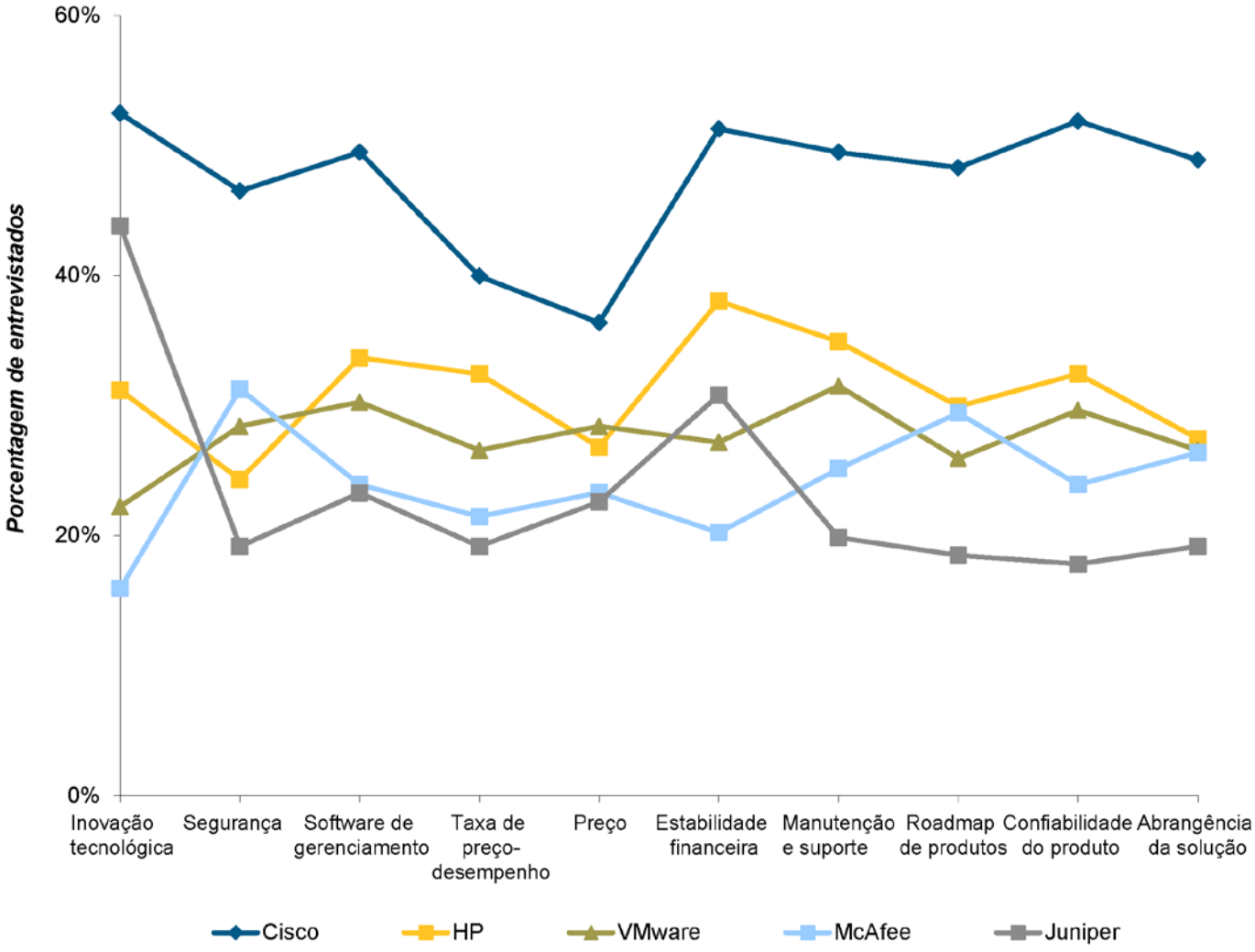
LIDERANÇA DOS FORNECEDORES DE SOLUÇÕES DE SEGURANÇA DE DATA CENTER

Perguntamos aos entrevistados o nome dos 3 principais fornecedores de soluções de segurança de data center para cada um dos 10 critérios de compra mais importantes (essa é uma questão proposta; os entrevistados poderiam selecionar somente dentre os 11 fornecedores que constam na lista). O gráfico a seguir mostra a porcentagem de entrevistados que consideram que cada fornecedor está entre os 3 primeiros de cada critério.

Como esse tipo de pergunta tende a favorecer fornecedores reconhecidos, e para eliminar a parcialidade da amostra, ajustamos a porcentagem de entrevistados com base na experiência de nossa amostra com cada fornecedor. O próximo gráfico inclui os 5 fornecedores mais citados.

A Cisco se saiu muito bem no geral (sua pontuação mais baixa ainda é maior do que a pontuação mais alta de qualquer outro), e sabemos que muitos compradores optam pela Cisco por ela ser uma parceira estratégica com uma grande visão que envolve mais do que apenas segurança. Em 2012, a Cisco lançou um novo conjunto de soluções com enfoque em data center e que recentemente integrou totalmente os produtos da Sourcefire. A principal falha da Cisco ao oferecer soluções de segurança para data centers de provedores de serviço é a falta de um produto de mitigação de DDoS, mas esperamos que eles a corrijam em breve.

Documento 8 Liderança de fornecedores de soluções de segurança de data center n=137



AUTOR DO RELATÓRIO

Jeff Wilson

Diretor de pesquisa, Tecnologia de segurança cibernética
IHS Infonetics
+1 408.583.3337 | jeff.wilson@ihs.com
Twitter: @securityjeff

SOBRE A IHS INFONETICS RESEARCH

Infonetics Research, agora parte da IHS (NYSE: IHS), é uma empresa de pesquisa de mercado e análise de consultoria internacional que atende ao setor de comunicações desde 1990. Líder na definição e rastreamento de tecnologias em desenvolvimento e estabelecidas em todo o mundo, a Infonetics ajuda os clientes a planejar, criar estratégias e competir com mais eficiência.

REIMPRESSÕES DO RELATÓRIO E PESQUISA PERSONALIZADA

Para obter informações sobre a distribuição de resumos de relatórios ou a pesquisa personalizada da IHS Infonetics, entre em contato com:

Américas:
+1 855 323-3363
+1 719 265-1535
Technology_US@ihs.com

Europa, Oriente Médio, África (EMEA):
+44 1344 328300
Technology_EMEA@ihs.com

Ásia-Pacífico
+604 291-3600
Technology_APAC@ihs.com